UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVID DE MEDICIS, on behalf of himself and all others similarly situated, Plaintiff, vs. ALLY BANK and ALLY FINANCIAL INC., Defendants.	**Civil Action No.: 21-cv-6799-NSR** **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff David De Medicis ("Plaintiff"), on behalf of himself and all others similarly situated, alleges as and for his Amended Class Action Complaint, the following against Ally Bank and Ally Financial Inc. ("Ally Financial") (collectively, "Ally" or "Defendants"), based upon his personal knowledge with respect to himself and his own acts, and upon information and belief as to his investigation and the investigation of his counsel as to all other matters:

SUMMARY OF THE ACTION

1. Beginning on or before February 18, 2021, and continuing until April 12, 2021, when Plaintiff and Class members used the Ally website customer portal to log in and access their Ally Bank accounts, Ally disseminated Plaintiff's and Class member's confidential usernames and passwords ("Sign-in Credentials") in clear unencrypted text to unauthorized recipients without the Plaintiff's or Class members' knowledge or consent (the "Breach").

2. For months Ally recklessly or negligently failed to take reasonable steps to test or monitor the operation of Ally's website to assure the security of Plaintiff's and Class member's Sign-in Credentials.

3. The Sign-in Credentials Ally disseminated in the Breach were linked to an array of other personal and confidential information Plaintiff and Class members entrusted to Ally associated with their Ally Bank accounts including, among other things: (a) full names and physical addresses; (b) email addresses; (c) account numbers; (d) current account balances; (e) checking account statements; (f) savings account statements; (g) investment account statements; (h) images of all cancelled checks; (i) names of account beneficiaries; (j) birth dates of account beneficiaries; (k) employment information; (l) the names of bank accounts linked to Ally Bank accounts; (m) last four digits of account numbers of bank accounts linked to Ally Bank accounts; (n) IRS tax forms; (o) last four digits of Social Security numbers; (p) Zelle account information; (q) and Zelle transaction history ("Private Information").

4. The Breach damaged the Plaintiff and Class members and subjected Plaintiff and Class members to imminent risk of harm.

5. Ally knew or must have known that bank sign-in credentials and other private information are regularly sold to identity thieves and other malicious actors on black markets such as on the dark web.

6. Nonetheless, Ally recklessly, or at the very least negligently, failed to take reasonable measures to maintain the confidentiality of Plaintiff's and Class member's Sign-In Credentials and Private Information.

7. Had Ally reasonably tested or monitored the operation of its website, Defendants could have warned Plaintiff and Class members that the Ally website did not provide secure access to their Ally Bank accounts and that merely logging in to their Ally Bank accounts using the Ally website created a significant risk that Ally would disseminate their Sign-in Credentials to strangers.

8. Alternatively, reasonable monitoring or testing would have made clear to Ally that its website was not functioning as Ally or Ally customers intended and Ally could have taken its website offline for repairs and prevented the website from ever disseminating Plaintiff's and Class member's Sign-in Credentials to unauthorized recipients.

9. Not only did Ally recklessly disregard or neglect to reasonably test or monitor the operation of its website, for *two months* Ally disseminated the Sign-in Credentials of unsuspecting Class members in clear unencrypted text to unauthorized strangers.

10. To corroborate that Ally's months-long Breach could have been entirely avoided had Ally merely reasonably tested or monitored its website, Ally represents that on April 12, 2021, Ally repaired the website so it no longer disseminated customer's unencrypted Sign-in Credentials to strangers, the very same day Ally claims it first became aware that its website was malfunctioning.

11. Despite Ally's legal obligation to give notice of the Breach without unreasonable delay, Ally withheld disclosing the Breach for two additional months, from April 12, 2021 until June 11, 2021, to develop a public relations strategy intended to minimize any competitive or reputational fallout from disclosure of the reckless conduct that caused the Breach.

12. Ally began mailing breach notification letters to Plaintiff and other Class members victimized by the Breach on or after June 11, 2021 ("DB Letter"). The June 11, 2021 DB Letter states that contrary to Ally's privacy policies and assurances that customer's Sign-in Credentials and related Private Information will be kept confidential, Ally disseminated Plaintiff's and Class member's Sign-in Credentials to unauthorized recipients.

13. The DB Letter also advised Plaintiff and Class members of steps to take for the coming 12 to 24 months in order to mitigate increased risk of identity theft caused to them by the Breach.

14. Predictably, soon after the Breach, fraudsters targeted customer's Ally Bank and associated online accounts. For example:

- On April 19, 2021, an Ally customer posted that an unauthorized transaction was made through his Ally Bank account at a Home Depot store the customer had never visited.[1]
- On May 3, 2021, an Ally customer posted that $3,000 in securities were taken from the customer's account.[2]
- On August 11, 2021, an Ally customer posted that, a few months earlier, he had incurred late payment fees because several bill payments with the customer's Ally debit card were declined after receiving a fraud alert from Ally.[3]
- On October 19, 2021, an Ally customer posted he had received an inquiry from Ally to confirm the customer changed the email address associated with the customer's Ally Bank account from yahoo to hush mail. The customer replied that he did not make the email change and Ally locked the customer's account. The customer was informed that

---

[1] https://www.depositaccounts.com/banks/reviews/ally-bank.html#:~:text=Never%20Have%20An,about%20their%20customers (last visited October 11, 2022).

[2] https://www.bbb.org/us/pa/ft-washington/profile/bank/ally-bank-0241-133953058/complaints?page=10#:~:text=05/03/2021,a%20financial%20institution (last visited October 11, 2022).

[3]https://www.consumeraffairs.com/finance/ally_bank.html#:~:text=Lucas%20of%20Tracy,hold%20of%20anyone.

Ally security would call but after 5 days never did. The customer was forced to pay bills with an account at a different bank.[4]

15. Malicious actors also repeatedly targeted Plaintiff's Ally Bank and associated online accounts causing Plaintiff to suffer financial and other damages.

16. In or about August 2022, well within the 12 to 24 months that Ally warned customers to lookout for identity theft caused by the Breach, a wave of thousands of unauthorized charges to Ally Bank customer debit and credit cards occurred further evidencing malicious actors' misuse of Private Information compromised by the Breach.

17. A lapse in time between a data breach and malicious actors' misuse of compromised information is not uncommon. Damage to Class members caused by misuse of Private Information occasioned by the Breach is far from over as evidenced by the latest wave of malicious attacks and continuing burden imposed upon the Plaintiff.

18. On behalf of himself and all those similarly situated, Plaintiff seeks the assistance of the Court to determine and award Plaintiff and Class members the proper amounts of damages Defendants' wrongful conduct has caused them to suffer and to award such other relief that the Court deems just and proper.

PARTIES

19. Plaintiff David De Medicis is a Virginia resident and maintains checking, savings, and securities accounts with Defendant Ally. Ally sent Plaintiff a DB Letter dated June 11, 2021

[4] https://www.depositaccounts.com/banks/reviews/ally-bank.html#:~:text=or%20NCUA%20insured.-,Banks,had%20to%20pay%20my%20credit%20card%20bill%20with%20my%20other%20bank,-Comments%20(1) (last visited October 11, 2022).

acknowledging that Ally disseminated Plaintiff's confidential Sign-in Credentials linked to a variety of Plaintiff's associated Private Information to unauthorized recipients.

20. Defendant Ally Bank is a corporation organized under the laws of the state of Utah. Ally Bank maintains its headquarters at 200 W Civic Center Drive, Suite 201, Sandy, Utah 84070. Ally Bank is the direct banking subsidiary of Defendant Ally Financial. Ally Bank is registered as a foreign corporation in the state of New York (DOS ID 3066925) and maintains one of its key operating locations in New York, New York. Ally Bank is one of the country's largest branchless online-only banks with about 2.3 million customers and retail deposits exceeding $124 billion.

21. Defendant Ally Financial is a corporation organized under the laws of the state of Delaware and maintains its headquarters at 500 Woodward Avenue, Floor 10, Detroit, Michigan 48226 and its Corporate Center at 601 S Tryon Street, Charlotte, North Carolina 28202Ally Financial common stock is traded on the New York Stock Exchange under the symbol "ALLY." Ally Financial is registered as a foreign corporation in the state of New York (DOS 3834452) and regularly does business in New York. Ally Financial is registered as a bank holding company under the Bank Holding Company Act and a Financial holding company under the Gramm-Leach-Bliley Act.

JURISDICTION AND VENUE

22. This Court has jurisdiction over this Action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2) ("CAFA"). The amount in controversy exceeds $5,000,000, exclusive of costs and interest. At least one member of the putative Class is a citizen of a state different from that of Ally Bank and Ally Financial and therefore minimal diversity required under CAFA is present. There are more than 100 putative Class members.

23. This Court also has jurisdiction over this Action pursuant to 28 U.S.C. §1332(a), diversity jurisdiction, because (i) the amount in controversy exceeds $75,000 and (ii) the Plaintiff and each of the Defendants are citizens of different States.

24. This Court has personal jurisdiction over Ally Bank because it is registered as a foreign corporation in New York and regularly does business in this district. Ally Bank provides digital direct banking services and investment securities services to consumers throughout New York and, as such, has continuous and systematic contact with New York sufficient to provide it with the minimum contacts necessary to satisfy the principles of fair play and substantial justice and the requirements of New York's long-arm statute. Further, Ally Bank committed tortious acts within this district. Ally Bank purposefully availed itself of the law of New York.

25. This Court has personal jurisdiction over Ally Financial because it is registered as a foreign corporation in New York and regularly does business in New York. Ally Financial has continuous and systematic contact with New York sufficient to provide it with the minimum contacts necessary to satisfy the principles of fair play and substantial justice and the requirements of New York's long-arm statute. Ally Financial purposefully availed itself of the law of New York.

26. Venue is proper in this judicial district pursuant to 28 U.S.C. §1391(a) because Ally Bank committed a tortious act in this District and a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

27. Ally Bank grew out of the banking division of General Motors Acceptance Corp. ("GMAC"). GMAC, among other things, was a provider of financing to purchasers of vehicles manufactured by General Motors Company. In 2009, the banking division of GMAC became

the bank holding company named Ally Financial Inc. Ally Bank is the direct banking subsidiary of Ally Financial Inc.

28. Ally Bank is a branchless or virtual bank that obtains retail deposits directly from customers through internet, telephone, mobile, and mail channels. Ally Bank offers savings accounts, money-market accounts, checking accounts, Certificates of Deposits, Individual Retirement Accounts, trust accounts, credit cards, mortgages, auto loans and investment products. Ally also offers Zella® person-to-person payment services, eCheck remote deposit capture, and mobile banking.

29. At all times relevant to this complaint Ally actively solicited potential and existing customer use of the Ally website to open or maintain checking, savings, securities and other financial accounts with Ally Bank. Ally Bank used customer deposits to generate profits and fees from lending and providing other banking and financial services.

30. Ally customers, including Plaintiff and Class members, reasonably expected Ally to undertake all actions reasonably necessary to maintain the confidentiality of their Sign-in Credentials and the Private Information associated with opening and maintaining their Ally Bank accounts.

31. Upon information and belief, Ally personnel responsible for overseeing the operation and security of Ally's website and computer systems at issue are based in Charlotte, North Carolina at the Ally Corporate Center.

32. Ally's computer systems that process and store Plaintiff's and Class member's Sign-in Credentials and Private Information are in or around Charlotte, North Carolina.

33. For example, during the Breach, Donna Hart, Ally Financial Chief Information Security Officer, and Kimberly Genobles, former Ally Bank Chief Privacy Officer, each

maintained their principal offices in Ally's Charlotte, North Carolina facilities. Notably, in June 2021, Genobles left her position at Ally Bank at or about the time the Breach was publicly disclosed.

A. ALLY ACTED RECKLESSLY OR NEGLIGENTLY

1. Ally collected and stored Plaintiff's and Class Member's Sign-in Credentials and other Private Information on its computer systems

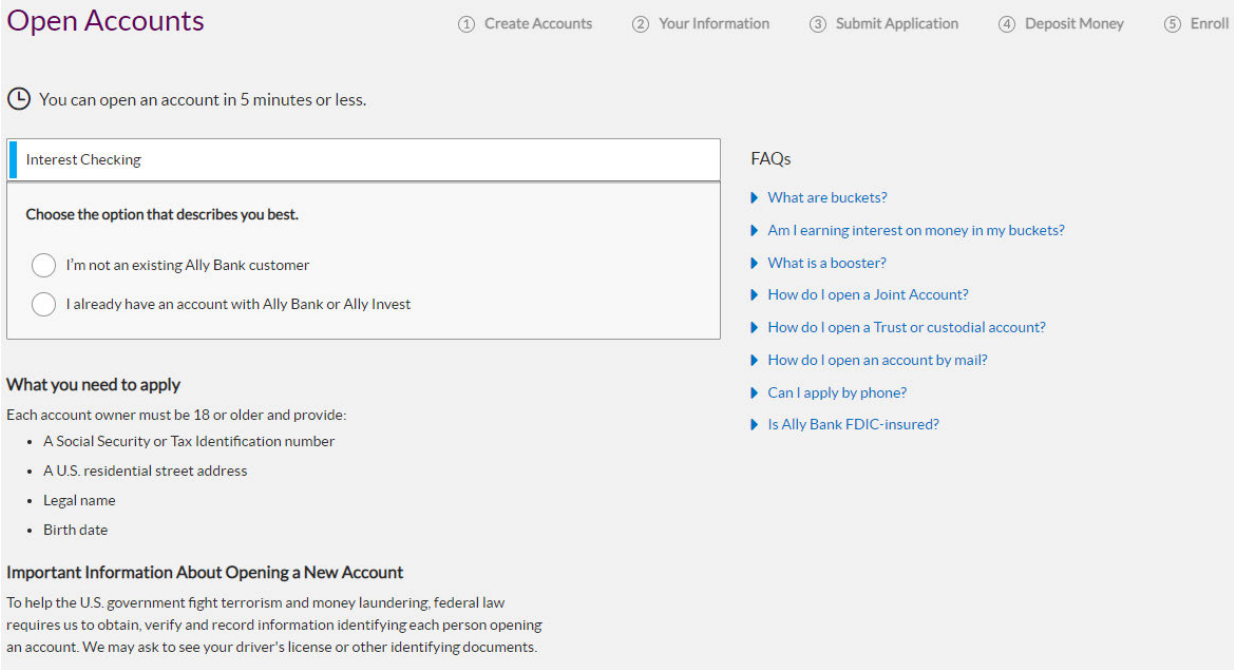
34. At all relevant times Ally solicited Plaintiff and Class members to open and or maintain financial accounts at Ally Bank.

35. Plaintiff and Class members each opened and or maintained financial accounts with Ally Bank using, among other things, Ally's website.

36. Ally required Plaintiff and Class members to provide Sign-in Credentials and other Private Information when opening and maintaining accounts at Ally Bank. Ally processed and stored Plaintiff's and Class member's Sign-in Credentials and Private Information on Ally's computer systems.

37. For example, Class Members could open an Ally Bank Interest Checking account accessing the Ally webpage below.[5]

[5] https://secure.ally.com/open-account/?OAP=DDA (last visited August 25, 2022).



38. When opening an Ally Bank Interest Checking account, customers were required to provide Ally with, among other things, a Social Security or Tax Identification number, U.S. residential street address, legal name, and birth date. Ally also collected driver's licenses and other identifying documents.

39. Ally collected similar Private Information from Plaintiff and Class members who opened and or maintained Ally Bank Savings accounts and Self-Directed Securities Trading accounts.[6]

[6] Ally Bank Savings online account application, https://secure.ally.com/open-account/?OAP=OSAV (last visited August 25, 2022) and Ally Invest Self Directed Securities Trading online account application, https://invest.ally.com/ola/?promo=CT61 (last visited August 25, 2022).

40. Ally also collected and stored Plaintiff's and Class members' Private Information when using the Ally website.[7]

Personal Information We Collect

We collect Personally Identifiable Information ("PII") about you from the information you provide to us when you visit our websites. The information we collect will depend on the Site you visit. This information may include, but is not limited to:

- Name
- Address
- Social Security number in whole or in part
- Phone numbers (including mobile)
- Account number
- Account number at a bank or other financial institution, type of bank account and the name of bank or other financial institution
- Demand Note number
- Email address
- Email referral information
- Date of birth
- Current residential information including mortgage or rent payments
- Employment information
- Income information
- Internet Protocol (IP) Address and/or domain
- Geo-location of your computer or mobile device
- Mobile carrier and/or Internet Service Provider

41. In connection with opening and or maintaining financial accounts at Ally Bank, Plaintiff and Class members each created confidential usernames and passwords, or Sign-in Credentials, to serve as their lock and key to prevent unauthorized access to their Ally Bank

[7] https://allyhomeloans.com/content/privacy-policy (last visited August 25, 2022).

accounts, assets in their Ally accounts, Private Information associated with those Ally accounts, and other financial accounts linked to their Ally Bank accounts.

2. Ally had an affirmative duty to undertake reasonable measures to maintain the confidentiality of Plaintiff's and Class Member's Sign-in Credentials and other Private Information

42. When Ally took possession of Plaintiff's and Class Members' Sign-in Credentials and other Private Information, Ally assumed an affirmative duty to take reasonable measures consistent with the banking industry to maintain the confidentiality of that information.[8]

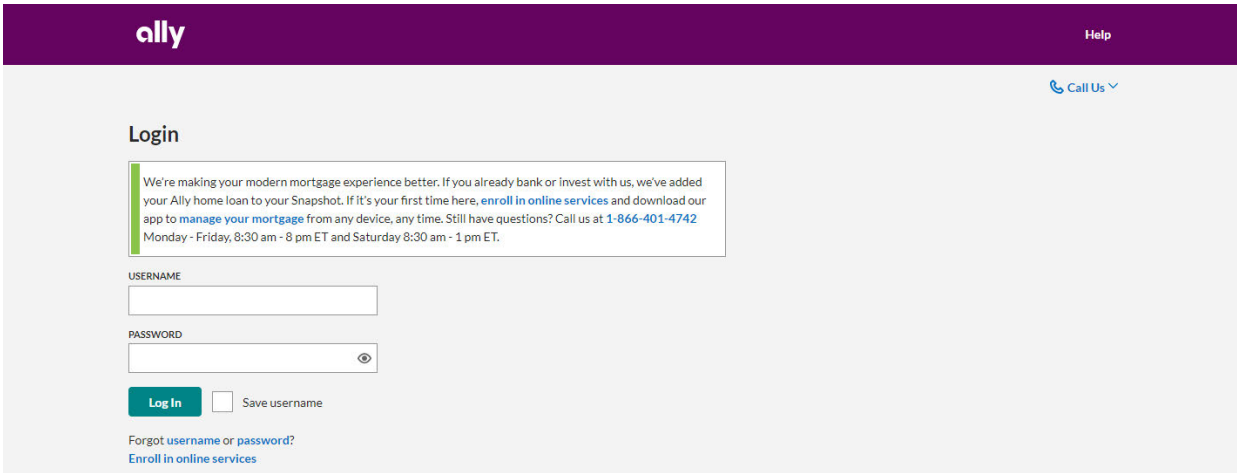
43. Likewise, when the Plaintiff and Class Members entrusted Ally with safeguarding their Sign-in Credentials and Private Information, they reasonably expected that Ally would not act recklessly or negligently in its handling, processing or storing that confidential information.

3. Ally recklessly or negligently failed to take reasonable steps to maintain the confidentiality of Plaintiff's and Class Member's Sign-in Credentials and Private Information

44. Plaintiff and Class members regularly access their Ally Bank accounts and other accounts linked to their Ally Bank accounts by entering their confidential Sign-in Credentials on the Ally website customer portal.

---

[8] *See e.g.*, *Council v. Dickerson's, Inc.*, 233 N.C. 472, 474-75, 64 S.E.2d 551, 553 (1951) (The law imposes upon every person who enters upon an active course of conduct the positive duty to exercise ordinary care to protect others from harm and calls a violation of that duty negligence. It is immaterial whether the person acts in his own behalf or under contract with another.); *Didato v. Strehler*, 262 Va. 617, 628, 554 S.E.2d 42, 48 (2001) ("[i]t is ancient learning that one who assumes to act, even though gratuitously, may thereby become subject to the duty of acting carefully, if he acts at all."); and *Boynton v. Kennecott Utah Copper, LLC*, 2021 UT 67, ¶ 29, 500 P.3d 847, 858 (Sup.Ct.) (Special relationships arise when one party assumes responsibility for the safety of another.)



45. On or before February 18, 2021, Ally began recklessly or, at a minimum, negligently operating its website such that when Plaintiff and other Class members input their Sign-In Credentials Ally disseminated those Sign-in Credentials in clear unencrypted text to unauthorized recipients who were complete strangers to Plaintiff and Class members.

46. Ally's reckless or negligent dissemination of Sign-In Credentials caused Plaintiff and Class members to suffer actual damage and or imminent risk of identity theft.

47. Beginning on or before February 18, 2021, continuing at least through April 12, 2021, Ally took no action to stop Defendants' unauthorized dissemination of Plaintiff's and Class member's unencrypted Sign-in Credentials.

48. Millions of customer log ins via Ally's malfunctioning website occurred during February 18 to April 12, 2021.

49. Not only were unencrypted Sign-in Credentials disseminated to unauthorized recipients, but those unauthorized recipients copied and stored the breached Sign-in Credentials onto their own computer systems.

50. Unauthorized recipients then further disseminated Plaintiff's and Class member's Sign-in Credentials to additional unauthorized recipients.

51. Because Defendants allowed the Breach to persist for months and during millions of customer log ins, formal discovery and investigation will likely shed light on the true extent that Sign-in Credentials and related Private Information were wrongfully disseminated and re-disseminated.

4. Black markets for compromised private information

52. Identity thieves and malicious actors covet stolen or misappropriated bank account sign-in credentials that are regularly marketed on the dark web. Fraudsters pay between $50 to $1,000 per bank account sign-in credential depending on the account balance.[9] The higher sign-in credential's account balance the higher the price fraudsters are willing to pay for that sign-in credential on the dark web.

53. Black markets also exist for the types of Private Information Plaintiff and Class members provided Ally in connection with opening, maintaining and transacting with their Ally Bank accounts.[10]

54. The Ally Breach compromised the security of precisely the types of private information criminals look to acquire and sell or use to commit crimes such as identity theft. *See e.g.*, ¶¶ 3, 38 and 40.

---

[9] https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/ (last visited August 25, 2022); https://www.zdnet.com/article/the-dark-web-how-much-is-your-bank-account-worth/ (last visited August 25, 2022); and https://www.watchguard.com/wgrd-news/blog/black-market-credentials-more-active-ever (last visited August 25, 2022).

[10] https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html (last visited August 25, 2022).

B. ALLY BREACHED IMPLIED AGREEMENTS WITH PLAINTIFF AND CLASS MEMBERS

55. Ally's unauthorized and wrongful dissemination of Plaintiff's and Class members' Sign-in Credentials violated a core principle of Ally's understanding and business relationship with its customers – Ally's obligation to safeguard the assets and confidential information customer's entrust Ally to safeguard.

56. Ally's repeated incontrovertible statements confirmed and reinforced this mutual understanding between Ally and its customers, including the Plaintiff and Class members.

1. "[W]e never share your usernames and passwords with anyone"

57. Ally stated on the Security page of its website under the heading "Credential Confidentiality" that "[W]e never share your usernames and passwords with anyone . . ."[11]

58. Not so. As described above, for months Ally wrongfully disseminated Plaintiff's and Class members' usernames and passwords, Sign-in Credentials, to unauthorized recipients.

59. Neither the Plaintiff nor the Class members authorized Ally to disseminate, or share, their Sign-in Credentials to those unnamed strangers.

2. "[O]nly people who need your information to do their jobs have access to the personal information you provide us."

60. Ally stated on its website that: "For your protection, only people who need your information to do their jobs have access to the personal information you provide us."[12]

61. Not true. Plaintiff and Class members entrusted Sign-in Credentials and other Private Information to Ally.

---

[11] https://www.ally.com/security/our-approach/ (last visited August 26, 2022).

[12] *Id*.

62. For months Ally wrongfully disseminated Plaintiff's and Class member's Sign-in Credentials to people who had no legitimate need for that personal information to do their jobs. Those Sign-in Credentials provide access to an array Plaintiff's and Class member's Private Information.

63. Strangers who had no need for Plaintiff's and Class member's Sign-in Credentials copied and then further disseminated that confidential information to additional unauthorized strangers who had no need for Plaintiff's or Class member's Private Information.

3. "[Ally uses] the latest encryption technology to help protect your information"

64. Ally stated "We use the latest encryption technology to help protect your information . . ."[13]

65. Not so, at least with respect to customer Sign-in Credentials. The Sign-in Credentials Ally wrongfully disseminated when the Plaintiff and Class members logged in to the Ally website were not protected with the latest encryption technology.

66. Rather, Ally transmitted Plaintiff's and Class members' Sign-In Credentials through the Internet in clear unencrypted text. In other words, no encryption technology at all.

4. Ally provides "a secure connection with your [Internet] browser when you log in"

67. Ally stated that its website provided "a secure connection with your [Internet] browser when you log in, complete an application, or enroll in online services."[14]

68. Not so. Ally omitted to disclose that merely logging in via Ally's unsafe and unsecure website led to the wrongful dissemination of Plaintiff's and Class member's Sign-In

[13] *Id.*

[14] *Id.*

Credentials to unauthorized recipients compromising the security of all their assets and Private Information.

5. "Keeping your accounts and personal information secure is a top priority for us."

69. Ally represented that "Keeping your accounts and personal information secure is a top priority for us."[15]

70. But Ally's "top priority" statement is belied by the fact that for nearly two full months, and during millions of unsecure customer logins, Ally utterly failed to monitor the operation of its website or to take any steps to stop disseminating confidential Sign-In Credentials to unauthorized recipients.

71. Had the security of Plaintiff's and Class members' confidential information in fact been a top priority, Ally would not have allowed the Breach to persist unabated for months.

6. Ally repeatedly warned customers of the critical need to maintain the confidentiality of Sign-in Credentials and Private Information

72. Ally's months-long Breach is particularly egregious given Ally's repeated admonitions directed to customers to ***never disclose passwords, usernames and other personal details when money is involved***.

73. Ally stated:

> **Protect your passwords.** Be cautious about your usernames and passwords with people, companies and services – especially when your personal information and money are involved. Never store your passwords in a note, memo or file on your computer or mobile device.[16]

* * *

[15] https://www.ally.com/security/ (last visited October 11, 2022).

[16] https://www.ally.com/security/password-security-tips.html (last visited July 11, 2021).

> Think carefully before you provide personal details on social networks like Facebook, Twitter and LinkedIn. **Never share information that financial institutions might use to identify you** like your Social Security number (including the last 4 digits), date of birth, personal phone number, home address, where you were born or schools you attended. Criminals might use this information to gain access to your account or use it to open accounts in your name (emphasis original).[17]
>
> * * *
>
> Always shred documents that contain personal information instead of placing them in your trashcan or recycling bin . . . **Criminals look for personal information in trashcans and use it to access your accounts or open new accounts** using your identity (emphasis original).[18]

74. Ally stated: "We never share your usernames and passwords with anyone – and ***we strongly recommend you don't share them either***."[19]

C. ALLY'S FAILURE TO MAINTAIN THE CONFIDENTIALITY OF PLAINTIFF'S AND CLASS MEMBERS' SIGN-IN CREDENTIALS AND OTHER PRIVATE INFORMATION CAUSED HARM TO PLAINTIFF AND THE CLASS

75. Ally's wrongful unauthorized dissemination of customer Sign-in Credentials caused harm to the Plaintiff and Class members in several ways.

1. Ally unexpectedly froze Plaintiff's Ally Bank accounts

76. On or about August 18, 2021, until August 27, 2021, Ally froze the Plaintiff's Ally Bank accounts and prohibited Plaintiff from accessing his funds on deposit in those accounts.

---

[17] https://www.ally.com/security/social-media-safety.html (last visited October 11, 2022).

[18] https://www.ally.com/security/how-to-protect-yourself-offline.html (last visited July 11, 2021).

[19] https://www.ally.com/security/our-approach/ (last visited October 11, 2022).

77. But for the Breach, the freezing of Plaintiff's Ally Bank accounts was entirely unexpected.

78. Prior to the Breach, Ally had never frozen Plaintiff's accounts.

79. Notably, Ally's website states that a bank's unexpected freezing of an account is a warning sign of fraud.

2. Freezing Plaintiff's Ally Bank accounts caused Plaintiff to lose opportunity and to suffer monetary damage

80. Ally's freezing of Plaintiff's accounts prohibited Plaintiff from transferring funds on deposit in his Ally Bank checking/savings account to his Ally Invest securities trading account.

81. Plaintiff uses cash deposits in his Ally Bank account to fund purchases in his Ally Invest securities trading account.

82. Ally's freezing of Plaintiff's accounts robbed the Plaintiff of the opportunity to purchase securities at advantageous market prices such as the Vanguard Russell 1000 Growth ETF.

83. When Ally finally permitted Plaintiff to access his cash deposits the favorable market prices that Plaintiff intended to make securities purchases were gone.

84. Prohibiting Plaintiff from using cash on deposit in his Ally Bank accounts caused the Plaintiff financial harm in losing the opportunity to purchase securities at favorable market prices.

3. Attempt to break into Plaintiff's Ally Bank accounts

85. On September 11, 2021, Ally emailed the Plaintiff alerting the Plaintiff that an unauthorized attempt to break into Plaintiff's Ally Bank accounts.

86. Prior to the Breach, Plaintiff is not aware of any unauthorized attempts to gain access or break into his Ally Bank accounts.

4. Hackers repeatedly attempt to take over Plaintiff's email account

87. Shortly after September 11, 2021, malicious hackers purportedly from Russia and the Netherlands began repeated attempts to sign in, gain access to, and take over Plaintiff's personal email account.

88. Prior to the Breach, Plaintiff is not aware of any unauthorized attempts to log in, improperly access and take over his personal email account.

5. Hackers make several attempts to access Plaintiff's FanDuel account

89. On November 16, 2021, the FanDuel Support Team notified the Plaintiff of multiple malicious attempts to break into Plaintiff's FanDuel account.

90. As a result of the repeated break in attempts, FanDuel froze Plaintiff's FanDuel account and prohibited Plaintiff from logging on or otherwise accessing his FanDuel account.

91. The freezing of Plaintiff's FanDuel account was unexpected.

92. Prior to the Breach, Plaintiff is not aware of any unauthorized attempts to log in and access his FanDuel account.

6. Repeated targeting of Plaintiff's online accounts with hacking, takeover attempts and other misuse has forced Plaintiff to devote substantial time to mitigate and remediate the adverse effects of the Breach

93. The imminent threat of identity fraud compelled the Plaintiff to devote many hours of time to ascertain, mitigate and remediate the Breach's adverse impacts on his privacy, his identity, and security of his financial and other accounts.

94. The Ally Breach has compelled Plaintiff to devote more than 20 hours of his time to ascertain, address and mitigate acts taken by fraudsters against his accounts and to address the imminent threat of future harm.

95. Among other things, the Breach forced Plaintiff to devote time to verify the legitimacy of the DB Letter, explore credit monitoring and identity theft insurance options, monitor his accounts for identity theft, communicate with Ally Bank via email and phone to regain access to his frozen Ally Bank accounts, address numerous unauthorized log in attempts to his email account, communicate with FanDuel via email and phone to regain access to his FanDuel account.

96. The many hours the Breach required Plaintiff to expend is lost and cannot be recaptured.

97. In addition to time, the Breach has also caused Plaintiff annoyance, inconvenience and anxiety due to increased concerns for the loss of his privacy.

7. The Breach continues to damage the Plaintiff and Class members and poses imminent threat of future harm

98. A wave of many thousands unauthorized transactions on Ally Bank debit and credit cards commenced in August 2022. Some of those unauthorized charges were to debit and credit cards that had never been activated or previously used.

99. The scale of fraudulent activity began to come to light when on Thursday, August 11, 2022, Ben Langhofer, a Wichita, Kansas financial planner, received a call from a woman in California claiming her account was used to make a fraudulent charge payable to myfamilyhandbook.com, Langhofer's small side business.[20]

[20] myfamilyhandbook.com markets customizable mission statements, core value statements and similar documents for families.

100. When Langhofer checked with the payment vendor, Stripe[21], used to process online payments for myfamilyhandbook.com orders he discovered an extraordinarily large number of transactions, nearly 800, and that each transaction was for $1, primarily from purported Ally Bank card holders.[22]

101. Langhofer inquired about the $1 transactions and Stripe explained that myfamilyhandbook.com had apparently been used by fraudsters for card testing, an online scheme in which fraudsters test improperly obtained credit card or debit card account numbers with small e.g., $1 charges to ascertain whether a stolen account is valid.

102. Fraudsters initially use small transaction amounts to avoid cardholder detection. Once an account is determined valid, fraudsters use the account for larger dollar transactions.

103. Days later, on Monday, August 15, 2022, Langhofer again checked the myfamilyhandbook.com payment processing account and discovered nearly 11,000 transactions, each for $1, primarily on Ally Bank cards initiated by email addresses minutely different from one another.

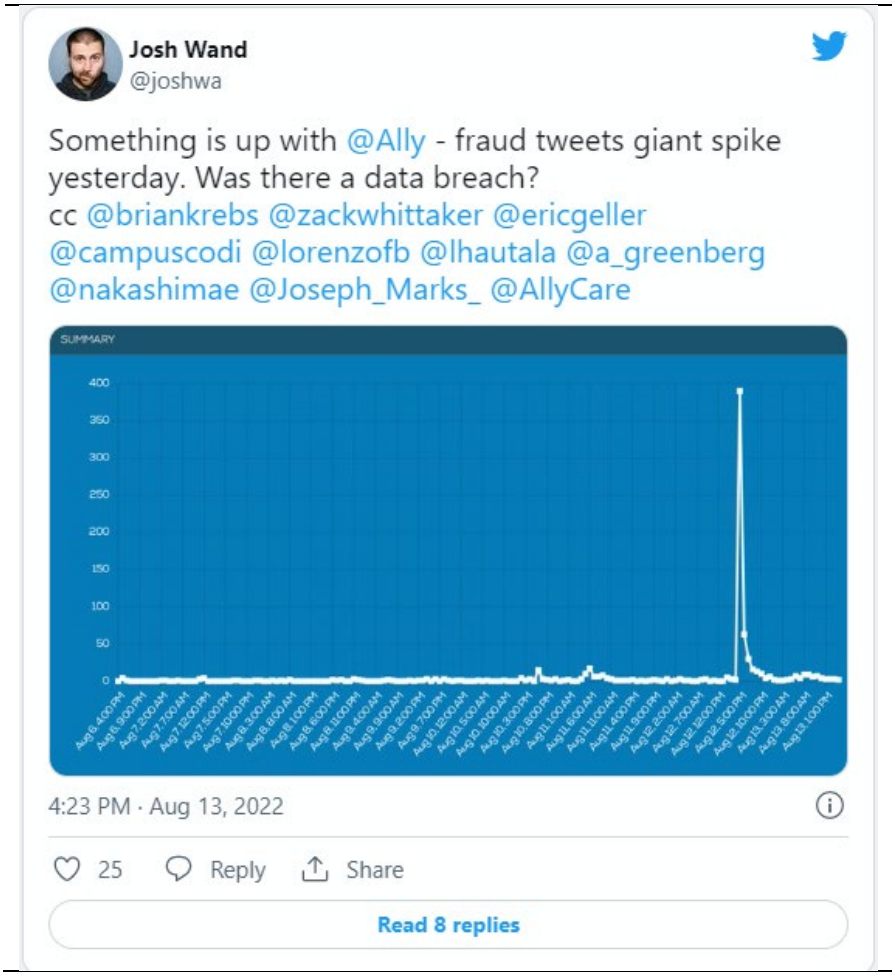
104. These thousands of unauthorized transactions demonstrate misuse of improperly procured data in large amounts from the Ally Breach and, a *fortiori*, a hallmark of the Breach relating to Ally accounts.

105. A giant spike in fraud tweets on r/AllyBank subreddit began in or around August 12, 2022, to which Twitter contributor, Josh Wand, wrote, "Was there a data breach?"

---

[21] https://Stripe.com (last visited January 6, 2023).

[22] https://arstechnica.com/information-technology/2022/08/wave-of-debit-card-fraud-hits-ally-bank-customers-hacked-vendors/ (last visited October 11, 2022).



106. A sampling of posts by Ally customers reporting fraudulent transactions on their Ally Bank accounts include:

> xues_1 mo. Ago
>
> Both me and wife's Ally debit card (2 diff accounts) had fraud charges on it on 8/15/2022. I use a bunch of different credit cards for reward hacking... never use my debit and keep it locked, so it got denied, but the card lives in a drawer and is never used... Ally has a breach. I have 2 other Mastercard accounts on credit and no issue... wonder if it's related to the April 2021 Ally breach lawsuit?[23]

* * *

[23]https://www.reddit.com/r/AllyBank/comments/wn4qs5/is_the_ally_data_breach_limited_to_debit_card/

Dodgerneighbor 1 mo. Ago

A review of Twitter account @AllyCare "Tweets & replies" today shows many fraud complaints and problems accessing the help line.

We were hacked.[24]

* * *

Speciator 1 mo. Ago

Yeah, it's crazy. Just locked my debit card and I got four notifications of blocked transactions from the thief attempting to use my card within the past hour.[25]

* * *

Youngcathiewood 26 days ago

My debit cards were charged at least a dozen times. When I noticed, it took me about 4 days to get a hold of an actual person to talk to about it. I couldn't get through on the phone after being on hold for an hour multiple times, it took half a day for my chat messages to get a response and by the time I would see it, they had already left the chat. Luckily they were nice enough to shipped overnight a new debit card that I just got yesterday. I ended up blocking certain types of purchases that the debit cards can be used for and I just got an alert about declined charges. I'm not sure if it was something that I have on auto pay or not, when I went to check the app the systems are down and I'm unable to log in. The charges on my card started around the 11th of August. Disappointing to say the least, I knew something was wrong right away because I never use my debit card or take it anywhere, it sits in my cabinet. The first thing I thought was data breach.[26]

Finished all my money out last week. So glad I did!

I had 6 checking accounts and 3 savings accounts with Ally for 5 years. Not really any major issues.

On the 9th of last month I had several fraudulent charges totaling $200 coming out of account number one. Called and took 10 days to get my money back

---

[24] *Id*.

[25] *Id*.

[26] https://www.reddit.com/r/AllyBank/comments/wn4qs5/comment/il65560/?utm_source=reddit&utm_medium=web2x&context=3 (last visited October 11, 2022).

Two weeks later I had a fraudulent $80 taken out of an account that had a zero balance and I'd never activated the debit card. Waited on hold an hour, took them two weeks to put the money back.

After seeing the issues from several others on this subreddit, I decided to lock all my cards and started moving my money/finances to a different bank. I'd already had accounts set up with SoFi and Capital360, so I transitioned to getting bills moved over to them.

I finally got everything moved this week and had only $60 left in my Ally accounts.

Today I got a notification that one of my Ally cards was declined for a $1 charge to a liquor store in NYC (I'm in the south).

I've had more fraudulent transactions in the last two months from one bank (but different checking accounts) than I've had in the previous 21 years I've been old enough to bank.

In fact, the only other times I've ever had a fraudulent charge, they were caught before they went through, declined and my bank called me! Not left it to me to notice and figure it out.

Besides the crappy situation, Ally has not told me (or anyone) about the issue, not disclosed that obviously Ally data has been breached in a way different than normal scamming, and their customer service is awful.

I'm so glad I've switched and I implore you all too as well. I've had great success with SoFi (used them for two years) and Capital360 and hoping to open a 3rd account with Discover when they open it back up to new applications.[27]

* * *

u/CB1826 5 days ago

Someone tried logging in to my Ally account

I thought this was limited to debit cards, but I woke up an email stating my online access has been locked due to multiple attempts with incorrect password or username. I literally just changed my password about 2 weeks ago.[28]

* * *

[27] https://www.reddit.com/r/AllyBank/comments/xaugmu/finished_all_my_money_out_last_week_so_glad_i_did/ (last visited October 11, 2022).

[28] https://www.reddit.com/r/AllyBank/comments/xbnhys/someone_tried_logging_in_to_my_ally_account/ (last visited October 11, 2022).

> UltimaCaitSith 4 days ago
>
> Got hacked, signed up with another bank, and quietly grumbling as we slowly transfer everything over. There's always a few autopay bills you forget about.[29]
>
> * * *
>
> RockyJayy 4 days ago
>
> I liked ally but with everything that happened recently and my old and newly issued card getting hit with fraud I moved banks.[30]

107. In response to the numerous reports of unauthorized transactions to Ally Bank accounts an Ally spokesperson acknowledged the increase in fraudulent activity caused by bad actors and that Ally's call centers were experiencing longer than usual wait times.

108. Likewise, the Plaintiff also experienced a wave of hacks and unauthorized transactions on his accounts.

109. On or before October 21, 2022, a malicious actor broke into the Plaintiff's Coinbase account using the password improperly disseminated in the Ally Breach. The fraudster then opened a Coinbase payment card account and spent down the total value of cryptocurrency then on deposit in Plaintiff's Coinbase account. The fraudster then initiated a $5,000 transfer of funds from Plaintiff's bank account at Wells Fargo to purchase $5,000 of Bitcoin in Plaintiff's Coinbase. The $5,000 Bitcoin purchase appears to be intended to enable the fraudster to make additional purchases with the fraudulent Coinbase payment card. Coinbase relied upon the fraudulent $5,000 transfer and executed the $5,000 Bitcoin purchase. Wells Fargo thereafter rejected the fraudster's transfer order because the Plaintiff did not have $5,000 available in his

---

[29] https://www.reddit.com/r/AllyBank/comments/xcs7xb/how_does_ally_have_so_many_bots_defending_it/

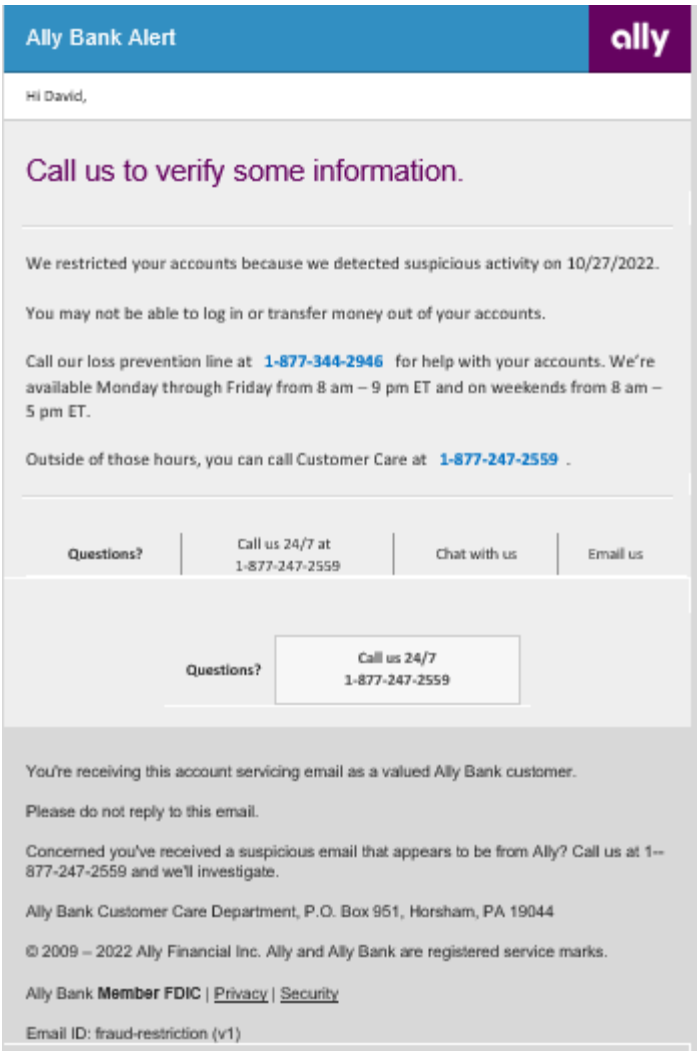
[30] *Id*.

Wells Fargo account at that time. Nonetheless, Coinbase held the Plaintiff liable for the $5,000 Bitcoin purchase. The market price of Bitcoin rose slightly after the $5,000 purchase and Coinbase confiscated the Bitcoin in Plaintiff's Coinbase account to cover the $5,000 transfer refused by Wells Fargo. Shortly thereafter the market price of Bitcoin dropped substantially. Had Coinbase confiscated the Bitcoin just days after it did, the Plaintiff would have been liable to Coinbase for difference in market value between the time of purchase and the time of confiscation.

110. The fraudster also appears to have attempted to transfer funds from Plaintiff's Ally Bank account to Coinbase also with a mind to make additional fraudulent purchases with the Coinbase payment card. As a result, Plaintiff's Ally accounts were shut down because of suspicious log ins and accounts were reopened with different account numbers. Again, during the fraud inquiry Ally prohibited the Plaintiff from accessing funds on deposit in his Ally Bank accounts.

111. Plaintiff's Ally Bank accounts and Coinbase account were linked because Plaintiff transferred money from his Ally Bank account to his Coinbase to initially fund the Coinbase account. In addition, the Plaintiff used the same password for his Ally Bank and Coinbase accounts prior to changing his Ally account password after the Ally Breach. Before the Breach, the Plaintiff's accounts with that password had never been hacked.

112. Coinbase eventually refunded to Plaintiff the amounts drawn down by the fraudster with the Coinbase payment card.



Ally Bank Alert

ally

Hi David,

Call us to verify some information.

We restricted your accounts because we detected suspicious activity on 10/27/2022.

You may not be able to log in or transfer money out of your accounts.

Call our loss prevention line at 1-877-344-2946 for help with your accounts. We're available Monday through Friday from 8 am – 9 pm ET and on weekends from 8 am – 5 pm ET.

Outside of those hours, you can call Customer Care at 1-877-247-2559 .

Questions?	Call us 24/7 at 1-877-247-2559	Chat with us	Email us

Questions? Call us 24/7 1-877-247-2559

You're receiving this account servicing email as a valued Ally Bank customer.

Please do not reply to this email.

Concerned you've received a suspicious email that appears to be from Ally? Call us at 1-877-247-2559 and we'll investigate.

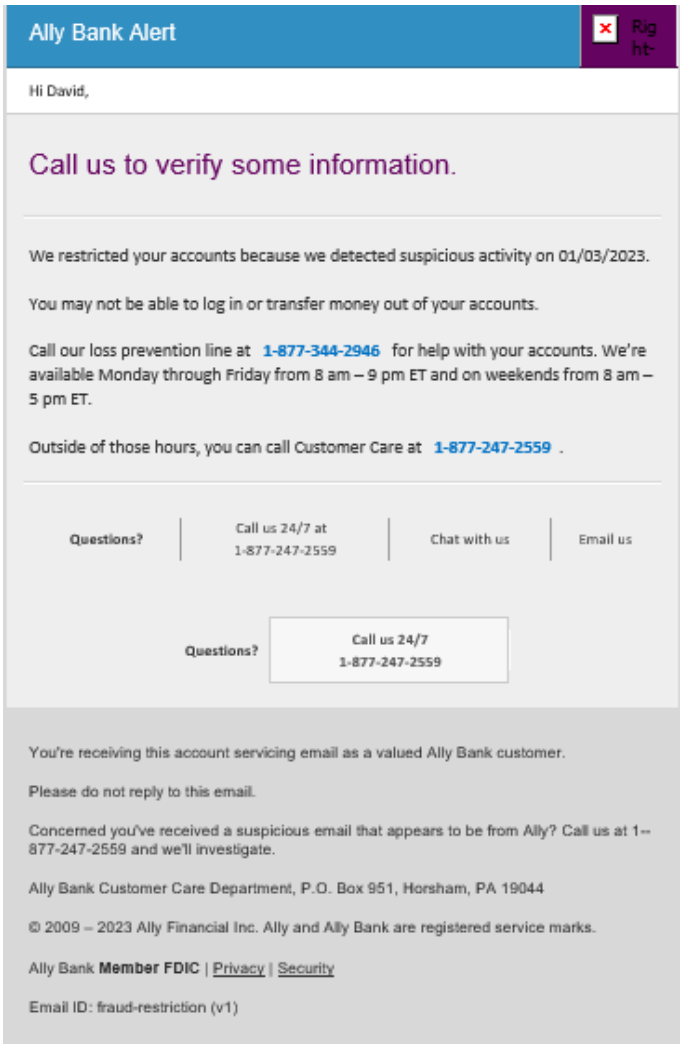
Ally Bank Customer Care Department, P.O. Box 951, Horsham, PA 19044

© 2009 – 2022 Ally Financial Inc. Ally and Ally Bank are registered service marks.

Ally Bank **Member FDIC** | Privacy | Security

Email ID: fraud-restriction (v1)

113. Since October 2022, Ally locked the Plaintiff out of his accounts because of suspicious activity on at least two additional occasions which required additional hours of Plaintiff's time to address. The Plaintiff received the most recent "fraud-restriction" email on January 3, 2023.



Ally Bank Alert

Hi David,

Call us to verify some information.

We restricted your accounts because we detected suspicious activity on 01/03/2023.

You may not be able to log in or transfer money out of your accounts.

Call our loss prevention line at 1-877-344-2946 for help with your accounts. We're available Monday through Friday from 8 am – 9 pm ET and on weekends from 8 am – 5 pm ET.

Outside of those hours, you can call Customer Care at 1-877-247-2559 .

Questions? | Call us 24/7 at 1-877-247-2559 | Chat with us | Email us

Questions? Call us 24/7 1-877-247-2559

You're receiving this account servicing email as a valued Ally Bank customer.

Please do not reply to this email.

Concerned you've received a suspicious email that appears to be from Ally? Call us at 1-877-247-2559 and we'll investigate.

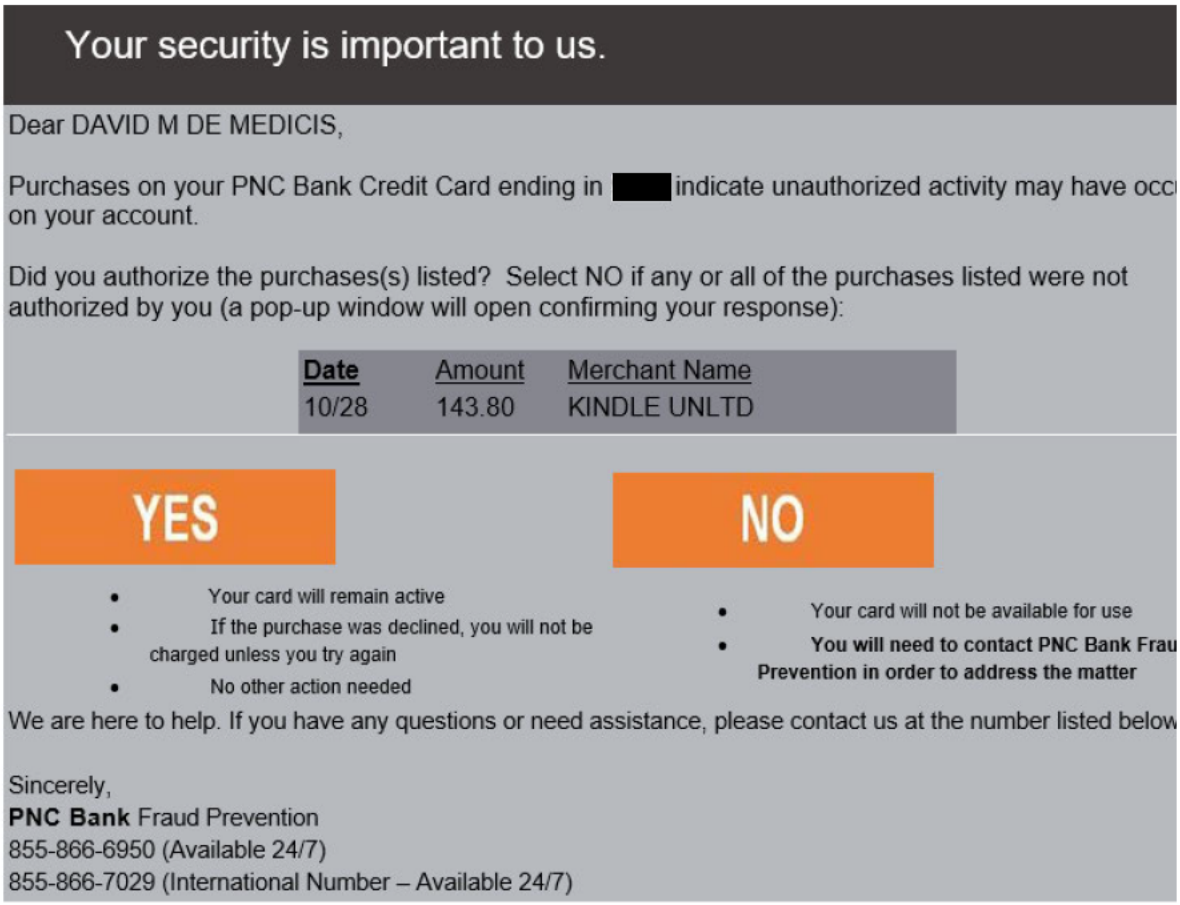
Ally Bank Customer Care Department, P.O. Box 951, Horsham, PA 19044

© 2009 – 2023 Ally Financial Inc. Ally and Ally Bank are registered service marks.

Ally Bank **Member FDIC** | Privacy | Security

Email ID: fraud-restriction (v1)

114. On or before October 28, 2022, a fraudster hacked Plaintiff's Amazon account using the password Ally disseminated in the Breach. The fraudster then attempted purchases using the Plaintiff's credit cards, including Plaintiff's PNC credit card linked to his Amazon account and that Plaintiff regularly paid using his Ally Bank account. For example, on October 28, 2022, the fraudster attempted to use Plaintiff's PNC credit card to purchase the subscription service Kindle Unlimited for $143.80 using Plaintiff's Amazon account but payment was rejected.



Your security is important to us.

Dear DAVID M DE MEDICIS,

Purchases on your PNC Bank Credit Card ending in [redacted] indicate unauthorized activity may have occ on your account.

Did you authorize the purchases(s) listed? Select NO if any or all of the purchases listed were not authorized by you (a pop-up window will open confirming your response):

Date	Amount	Merchant Name
10/28	143.80	KINDLE UNLTD

YES

- Your card will remain active
- If the purchase was declined, you will not be charged unless you try again
- No other action needed

NO

- Your card will not be available for use
- You will need to contact PNC Bank Frau Prevention in order to address the matter

We are here to help. If you have any questions or need assistance, please contact us at the number listed below

Sincerely,
PNC Bank Fraud Prevention
855-866-6950 (Available 24/7)
855-866-7029 (International Number – Available 24/7)

115. The fraudster was successful in making two unauthorized purchases on the Plaintiff's Chase Amazon Visa card. Amazon subsequently refunded the Plaintiff's account for those two fraudulent purchases.

8. Dissemination of Plaintiff's and Class member's unencrypted Sign-in Credentials creates an imminent risk of injury

116. As reflected by the wave of fraudulent transactions involving Ally Bank accounts, despite the lapse in time since the Breach was first publicly reported the risk of harm the Breach poses to Plaintiff and Class members is imminent.

117. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."

118. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

119. Moreover, there is often a time lag between when harm occurs versus when it is discovered, and between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

120. [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

121. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

122. The injuries to Plaintiff and Class members were directly and proximately caused by Ally's failure to implement or maintain adequate data security measures for its customers.

9. Ally implicitly admitted the Breach harmed Plaintiff and the Class

123. Ally implicitly acknowledged the Breach caused harm to Plaintiff and the Class subjecting them to heightened risk of identity theft when, "as a precautionary measure to help safeguard" Plaintiff and Class members, Ally offered 24 months of Equifax credit monitoring.

124. But Equifax does not fully protect Plaintiff from identity theft, and even if it did, 24 months is by no means a sufficient duration of credit monitoring given the breadth and extent of Private Information compromised in the Breach.

D. PLAINTIFF AND THE CLASS HAVE A CONTINUING INTEREST IN ENSURING THAT THEIR PRIVATE INFORMATION IN ALLY'S POSSESSION IS ADEQUATELY SAFEGUARDED FROM FUTURE BREACHES

125. Plaintiff and Class members have a continuing interest in ensuring that their Private Information in Ally's possession is adequately protected from future breaches.

126. It is well known that Private Information is highly coveted and a frequent target of fraudsters and identity thieves.

127. Legitimate organizations and the criminal underground alike recognize the value of Private Information contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it.

128. Nonetheless, Ally's readily avoidable, months long Breach reflects a lackadaisical, cavalier, reckless, or at the very least, negligent, approach to maintaining the privacy and security of the Plaintiff's and Class member's Private Information.

129. The Breach could have been prevented had Ally merely monitored and tested its website properly and engaged in standard data security practices such as encrypting Plaintiff's and Class members' Private Information.

130. Ally's inexcusable conduct that caused the Breach is exacerbated by the repeated warnings and alerts directed to financial institutions about the need to protect and secure computer systems.

131. Ally has not made any public statements to explain how the Breach was allowed to persist for two months and millions of customers log ins purportedly without detection.

132. Moreover, other than stating that its malfunctioning website was reprogrammed, Ally has not disclosed any remedial measures Ally has taken to ensure that Plaintiff and Class members will not be subjected to a similar, completely avoidable, security breaches in the future.

CLASS ALLEGATIONS

133. Pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Class defined as follows:

> All persons in the United States whose Sign-In Credentials were disseminated to unauthorized recipients in the Breach announced by Ally Bank on or about June 11, 2021.

134. The Class is so numerous that joinder of all members is impracticable. On information and belief, the Class has more than one million members. Among other things, Ally Bank has 2.33 million deposit customers and 425,000 investment brokerage accounts.

135. Disposition of claims of the Class in a single action will provide substantial benefits to the parties, Class members, and the Court.

136. Numerous questions of law and fact common to Plaintiff and members of the Class include, but are not limited to:

(a) whether Ally acted recklessly or negligently in operating its website such that Plaintiff's and Class member's Sign-in Credentials were disseminated to unauthorized recipients;

(b) whether an implied contract existed between Ally and Class members pertaining to the safeguarding of Sign-in Credentials and Private Information and, if so, whether Ally breached that implied contract;

(c) whether a fiduciary relationship existed between Ally and Class members pertaining to the safeguarding of Sign-in Credentials and Private Information and, if so, whether Ally breached its fiduciary duties to Class members;

(d) whether Ally unnecessarily delayed disclosing the Breach to Class members;

(e) the extent to which Class member's Sign-in Credentials and other Private Information was disseminated to unauthorized recipients and then further disseminated by unauthorized recipients to additional unauthorized recipients;

(f) whether lack of adequate controls and oversight at Ally enabled the Breach to occur and then to persist unabated for two months;

(g) the extent Plaintiff's and Class member's Private Information was improperly compromised or accessed because of the Breach; and

(h) the proper measure of damages the Breach had caused to Plaintiff and Class members.

137. Plaintiff's claims are typical of the claims of Class member's claims. Plaintiff and Class members suffered the same injury – *i.e.*, Ally compromised the security of Plaintiff's and Class member's Sign-in Credentials and Private Information.

138. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions.

139. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Class and have the financial resources to do so.

140. Neither Plaintiff nor his counsel have interests that are contrary to or that conflict with those of the proposed Class.

141. Common issues of law and fact arising from Ally's conduct predominate over any individual issues. Adjudication of these common issues in a single action will promote judicial economy.

142. A class action is the superior method for fair and efficient adjudication of this controversy. The interests of individual Class members in controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Ally Bank and Ally Financial.

143. Individualized litigation would present a potential for inconsistent or contradictory judgments, increased delay and expense to all parties and the court system.

144. Ally's records pertaining to the Breach will easily identify the Class members. Common documents and testimony will be used to prove Plaintiff's and Class member's claims.

145. The class action procedure here will have no management difficulties.

146. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Ally acted, or refused to act, on grounds that apply generally to Class members so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class members.

COUNT I

Negligence

147. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

148. Ally required Plaintiff and Class members to create and entrust Ally with Sign-in Credentials and other Private Information to open, use and maintain accounts at Ally Bank.

149. By collecting and storing this data, and using it for commercial gain, Ally assumed a duty of care to use reasonable means to secure and safeguard Sign-in Credentials and other Private Information and prevent unauthorized disclosure or misuse that information.

150. Ally's duties included a responsibility to implement procedures and practices to secure Sign-in Credentials and Private Information from inadvertent unauthorized disclosure, to promptly detect any such unauthorized disclosure or misuse, and give prompt notice to Plaintiff or any other Class member affected by any security breach.

151. Ally owed a duty of care to consistent with industry standards and to ensure that their websites, systems, networks, and the personnel responsible for them, adequately protected Plaintiff's and Class member's Sign-in Credentials and Private Information.

152. Only Ally was positioned to operate its website and to ensure that its website was safe for Plaintiff and Class members to use such that their Sign-in Credentials and Private Information entrusted to Ally were secure.

153. Ally breached its duty to Plaintiff and Class members by failing to take reasonable measures to protect Plaintiff's and Class member's Sign-in Credentials and associated Private Information.

154. The specific negligent acts and omissions committed by Ally include, but are not limited to, the following:

(a) operating its website for months in a manner that disseminated Plaintiff's and Class member's Sign-in Credentials to unauthorized recipients;

(b) failing to adequately test or monitor the operation of their website;

(c) failing to timely repair its malfunctioning website; and

(d) failing to timely notify Plaintiff and Class members of the malfunctioning website and Breach.

155. The Breach was a foreseeable result of Ally's lack of reasonable care in testing, monitoring, and operating the Ally website.

156. Injuries to Plaintiff and Class members caused by Ally's failure to reasonably test, monitor, or operate the Ally website were also foreseeable. Those injuries include actual monetary loss and economic harm, as well as ongoing, imminent, impending threat of identity theft, fraud, and abuse, resulting from loss of confidentiality of Private Information, the illegal sale of the compromised Private Information on black markets such as on the dark web, time spent scrutinizing bank statements, credit card statements, and credit reports, expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings, lost work time, and other economic and non-economic harm.

157. Accordingly, Plaintiff, individually and on behalf of all those similarly situated, seeks an order declaring Ally's conduct alleged herein constitutes recklessness or negligence, that Ally's conduct caused harm to Plaintiff and Class members, and an award of damages to Plaintiff and the Class in an amount to be determined at trial.

COUNT II

Negligence Per Se

158. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

159. Section 5 of the Federal Trade Commission Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade

Commission ("FTC"), the unfair act or practice by companies such as Ally's failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Ally's duty.

160. Ally violated Section 5 of the FTC Act (and similar state statutes) by failing to comply with industry standards to protect Sign-in Credentials and Private Information.

161. Ally's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

162. Plaintiff and the Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

163. The harm Ally caused Plaintiff and members of the Class to suffer is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC itself has pursued numerous enforcement actions against businesses which, due to their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused harm similar to the harm suffered here.

164. As a direct and proximate result of Ally's improper conduct, Plaintiff and members of the Class have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III

Breach of Implied Contract

165. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

166. Ally solicited and invited Plaintiff and Class members to provide their Private Information through Ally's website as part of its regular business practices. The Plaintiff and

Class members accepted Ally's offers and provided their Private Information to Ally. In entering such implied contracts, Plaintiff and Class members understood that Ally would undertake appropriate safeguards and data security practices and policies consistent with industry standards, and that Ally would use part of the fees paid by Plaintiff and the members of the Class to pay for adequate and reasonable data security practices.

167. Indeed, Ally made the aforementioned representations such as in Paragraphs 57 through 71, promising to safeguard and protect the Sign-in Credentials and Private Information of Plaintiff and each Class Member.

168. Plaintiff and Class members would not have used Ally's website or entrusted their Private Information with Ally in the absence of the implied contract between them and Ally to keep their Sign-in Credentials and other Private Information secure.

169. Plaintiff and Class members fully performed their obligations under the implied contract with Ally.

170. Ally breached their implied contract with Plaintiff and Class members by, among other things, failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice that their Sign-in Credentials were disseminated to strangers and their Private Information was compromised as a result of the Breach.

171. As a direct and proximate result of Ally's breaches of their implied contract, Plaintiff and Class members sustained actual losses and damages as described in an amount to be proven at trial.

COUNT IV

Breach of Fiduciary Duty

172. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

173. At all relevant times a fiduciary relationship existed and continues to exist between Plaintiff and Ally.

174. Ally possessed Plaintiff's Sign-in Credentials and Private Information that belonged to the Plaintiff and was confidential.

175. Ally disclosed Plaintiff's Sign-in Credentials to strangers without the Plaintiff's authorization and compromised the security of Plaintiff's Private Information.

176. Plaintiff was damaged by Ally's wrongful unauthorized disclosure of Plaintiff's Sign-in Credentials.

177. Ally's unauthorized disclosure of Plaintiff's Sign-in Credentials was a substantial factor in causing harm to the Plaintiff.

COUNT V

Violation of the North Carolina Unfair & Deceptive Trade Practices Act, N.C. Gen. Stat § 75-1.1, et seq.

178. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

179. In connection with the solicitation, promotion, offering, and rendering online banking services, Ally engaged in a pattern of unfair and/or deceptive acts or practices in violation of the North Carolina Unfair & Deceptive Trade Practices Act, N.C. Gen. Stat § 75-1.1.

180. Ally's unfair or deceptive acts and practices include but are not limited to making deceptive and misleading representations to consumers that:

a. "[W]e never share your usernames and passwords [Sign-in Credentials] with anyone . . ." when Ally's website disseminated customer Sign-in Credentials to unauthorized recipients;

b. "For your protection, only people who need your information to do their jobs have access to the personal information you provide us" when Ally's website disseminated customer Sign-in Credentials to unauthorized recipients giving access to personal information people had no need to do their jobs;

c. "We use the latest encryption technology to help protect your information . . . when Ally disseminated customer Sign-in Credentials to unauthorized recipients in clear unencrypted text;

d. Ally provided "a secure connection with your [Internet] browser when you log in, complete an application, or enroll in online services" when merely logging in to the Ally website customer portal resulted in dissemination of Plaintiff's and Class member's Sign-in Credentials to strangers; and

e. "Keeping your accounts and personal information secure is a top priority for us" when Ally failed to test or monitor the operation of its website such that its website disseminated Sign-in Credentials to unauthorized recipients for two months during millions of customer log ins.

181. Plaintiff entrusted Ally with his Sign-in Credentials and other Private Information and believed Ally would keep that information confidential.

182. Each of Ally's above statements was either not true or materially misleading.

183. Ally's representations and practices possessed the tendency and capacity to mislead Plaintiff and Class members or created the likelihood that Plaintiff and Class members would be deceived.

184. Upon information and belief, Ally stored Sign-in Credentials of North Carolina residents that Ally wrongfully disseminated in the Breach.

185. Ally violated breach notification acts of North Carolina (N.C. Gen. Stat § 75-65), Virginia (Va. Code. Ann. §§ 18.2-186.6), and other similar state laws by its unreasonable two-month delay in providing notice of the Breach to Plaintiff and Class members.

186. Ally's acts and practices proximately caused Plaintiff's and Class member's damages.

COUNT V

Violation of the Virginia Personal Information Breach Notification Act, Va. Code. Ann. §§ 18.2-186.6, et seq.

187. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

188. Ally was required to accurately notify Plaintiff and Class members following discovery of a breach of its data security system if unencrypted or unredacted Private Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

189. Ally owns or licenses computerized data that includes personal information as defined by Va. Code Ann. § 18.2-186.6(B).

190. Plaintiff's and members of the Class's Private Information includes personal information as defined by Va. Code Ann. § 18.2-186.6(A).

191. Because Ally discovered a breach of its security system involving the Private Information of the Plaintiff and Class members that Ally stored, in which unencrypted or unredacted Private Information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Ally had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

192. Ally's failure to disclose the Data Breach in a timely and accurate manner, violated Va. Code Ann. § 18.2-186.6(B).

193. As a direct and proximate result of Ally's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Class members suffered damages, as described above.

194. Plaintiff and Class members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

COUNT VI

Injunctive / Declaratory Relief, Declaratory Judgment Act, 28 U.S.C. §2201

195. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

196. The Plaintiff and Class members entered an implied contract and fiduciary relationship with Ally Bank that obligates Ally to provide industry standard security for the Sign-in Credentials and Private Information Ally collects from Plaintiff and Class members and processes and stores on Ally's computer systems.

197. Ally owed, and continues to owe, Plaintiff and Class members a duty of care to secure their Sign-in Credentials and Private Information from access by unauthorized recipients and bad actors.

198. Ally continues to possess Plaintiff's and Class member's Sign-in Credentials and Private Information and stores and processes that information on Ally's computer systems.

199. For two months during the Spring of 2021, and millions of customer log ins, Ally wrongfully disseminated Plaintiff's and Class member's Sign-in Credentials to strangers.

200. The Breach was the product of reckless, or at a minimum, woefully inadequate data security practices and policies that also permitted the Breach to persist for two months.

201. Ally claims that the same day that Ally became aware that Ally had for two months disseminated its own customer's Sign-in Credentials to unauthorized recipients, Ally repaired its malfunctioning website to stop the wrongful dissemination of customer's Sign-in Credentials.

202. Nor is wrongful dissemination of customer's confidential information through third parties unique at Ally.[31]

203. Now many thousands of Ally customers are experiencing unauthorized transactions to their Ally Bank debit and credit accounts by fraudsters who improperly gained access to their Private Information.

204. Ally has announced very little in terms of changes to its security practices and infrastructure that caused the Breach to protect Plaintiff and Class members from further data security lapses leading to additional breaches.

205. There is no reason to believe that the Defendants' security practices are any more adequate now than at the time the Breach occurred.

---

[31] https://oag.ca.gov/system/files/Ally%20CA%20Customer%20Notification%20Letter_0.pdf (last visited October 11, 2022).

206. Plaintiff, therefore, seeks a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate security of Private Information, and (2) that to comply with their obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

b. Ordering that Defendants audit, test, and train their security personnel regarding existing, new or modified security procedures;

c. Ordering Defendants to not transmit Private Information in an unencrypted form on its website;

d. Ordering the Defendants to not share Private Information with third parties without the express written permission of Plaintiff and the Class;

e. Ordering Defendants to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

C. That the Court grant permanent injunctive relief to prohibit Ally from engaging in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiff and members of the Class compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Ally as a result of its unlawful acts, omissions, and practices;

F. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

G. That Plaintiff be granted the declaratory relief sought herein;

H. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

I. That the Court award pre- and post-judgment interest at the maximum legal rate; and

J. That the Court grant all such other relief as it deems just and proper.

Dated: January 9, 2023

KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.

/s/ Melissa R. Emert
Melissa R. Emert, Esq.
16 Squadron Boulevard, Suite 106
New City, NY 10977
memert@kgglaw.com
T: 845-356-2570
F: 845-356-4335

SLYNE LAW LLC
Patrick Slyne, Esq.
800 Westchester Avenue, N641
Rye Brook, NY 10573
Patrick.Slyne@SlyneLaw.com
T: (914) 279-7000
F: (914) 653-8122

SHUB LAW FIRM LLC
Jonathan Shub, Esq.
134 Kings Highway East, 2nd Floor
Haddonfield, NJ 08033
jshub@shublawyers.com
T: (856) 772-7200
Attorneys for the Plaintiff and Members of the Putative Class

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVID DE MEDICIS, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

ALLY BANK and ALLY FINANCIAL INC.,

Defendants.

Civil Action No.: 21-cv-6799-NSR

CERTIFICATE OF SERVICE

I hereby certify that on this 9th day of January, 2023, I electronically filed a true and correct copy of the foregoing ***AMENDED CLASS ACTION COMPLAINT*** with the Clerk of the Court using the CM/ECF system which sends notification to the attorneys of record who are duly registered with the CM/ECF System.

/s/Cherie Cornfield
Cherie Cornfield